

Vertrag über die Auftragsverarbeitung personenbezogener Daten (AV-Vertrag)

zwischen

Netzwerk Universitätsmedizin NUM GmbH
c/o Charité - Universitätsmedizin Berlin
Charitéplatz 1
10117 Berlin

(Verantwortlicher im Sinne der DS-GVO, nachfolgend „Auftraggeber“ genannt)

und

[...]

(Auftragsverarbeiter im Sinne der DS-GVO, nachfolgend „Auftragnehmer“ genannt)

Präambel

Dieser Auftragsverarbeitungs-Vertrag (AV-Vertrag) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Vertrag

[...]

(im Folgenden Hauptvertrag genannt) beschriebenen Auftragsverarbeitung ergeben.

Sämtliche in diesem Vertrag beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiterinnen und Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen bzw. kommen könnten.

§ 1 Definitionen

Es gelten die Begriffsbestimmungen entsprechend Art. 4 DS-GVO, § 2 UWG, § 2 TMG, Bundesdatenschutzgesetz (BDSG), Strafgesetzbuch (StGB) und Landesdatenschutzgesetz (BlnDSG) sowie Landeskrankenhausgesetz des Landes Berlin (BlnLKG). Sollten in den Artikeln bzw. Paragraphen sich widersprechende Darstellungen zu finden sein, gelten die Definitionen in der Rangfolge DS-GVO, Landesrecht, UWG/Geschäftsgeheimnisgesetz und TMG. Weiterhin gelten folgende Begriffsbestimmungen:

(1) Anonymisierung

Prozess, bei dem personenbezogene Daten entweder vom für die Verarbeitung der Daten Verantwortlichen allein oder in Zusammenarbeit mit einer anderen Partei unumkehrbar so verändert werden, dass sich die betroffene Person danach weder direkt noch indirekt identifizieren lässt. (Quelle: DIN EN ISO 25237)

(2) Pseudonymisierung

Im Sinne dieses Vertrages ist Pseudonymisierung die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

(3) Unterauftragnehmer

Vom Auftragnehmer beauftragter Leistungserbringer, dessen Dienstleistung und/oder Werk der Auftragnehmer zur Erbringung der in diesem Vertrag beschriebenen Leistungen gegenüber dem Auftraggeber benötigt.

(4) Weisung

Weisung ist die auf einen bestimmten Umgang (zum Beispiel Anonymisierung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche oder elektronische Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den jeweiligen Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher oder elektronischer Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2 Gegenstand des Auftrags

- (5) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Es werden keine sensiblen Daten im Sinne des Art. 9 Abs. 1 DS-GVO verarbeitet.

Dies umfasst Tätigkeiten, die im Hauptvertrag und in der darin enthaltenen Leistungsbeschreibung konkretisiert sind.

- (6) Die Verarbeitung der personenbezogenen Daten durch den Auftragnehmer erfolgt wie nachfolgend spezifiziert. Die Verarbeitung betrifft ausschließlich die fortfolgend bezeichneten Kategorien personenbezogener Daten, Kategorien betroffener Personen, Zwecke sowie Art und Umfang der Verarbeitung.

(7) Kategorien personenbezogener Daten

Nr.	Datenkategorien	Details zu Datenkategorien
1	Basis-Stammdaten	☐ Anrede ☐ Name, Vorname ☐ Geburtsdatum ☐ Anschrift ☐ Kontaktdaten ☐
2	Erweiterte Stammdaten	☐ Kontodaten ☐ Versichertendaten/Versicherungsnummer ☐
3	Sonstige Daten	☐ Audiodaten ☐ Videodaten ☐

(8) Kategorien betroffener Personen

Kategorien betroffener Personen	☐ Kunden ☐ Befragte ☐ Beschäftigte ☐ sonstige: [Bitte ergänzen]
--	--

(9) Zwecke der Verarbeitung

Zwecke	☐ Erfüllung eines Vertrages ☐ Verwaltungszwecke ☐ (Direkt)marketing ☐ Reparatur und Wartung ☐ Backup-Sicherheitspeicherung ☐ Entsorgung von Datenträgern ☐ weitere: [Bitte geben Sie die Zwecke der Verarbeitung an]
---------------	---

(10) Art und Umfang der Verarbeitung

[Bitte jeweils für den konkreten Auftrag beschreiben]

Art	☐ Erheben ☐ Erfassen ☐ Ordnen ☐ Speicherung und Aufbewahrung ☐ Anpassung oder Veränderung ☐ Auslesen und Einsicht nehmen ☐ Verbreitung oder eine andere Form der Bereitstellung ☐ Abgleich oder Verknüpfung ☐ Einschränkung, Löschen oder Vernichtung von Daten ☐ weitere: ...
Umfang	[welche Datenkategorien zu welchem Zweck]

- (11) Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Auftragsverarbeitungsvertrages.

§ 1 Ort der Datenverarbeitung

[Option 1: Verarbeitung innerhalb EU/EWR]

- (1) Die Parteien werden personenbezogene Daten im Rahmen der Durchführung des Projekts ausschließlich in den Mitgliedsstaaten der Europäischen Union oder in einem anderen Staat verarbeiten, der Partei des Vertrags über den Europäischen Wirtschaftsraum ist.
- (2) Absatz 1 gilt für den Einsatz von Auftragsverarbeitern gemäß § 11 entsprechend.

[ODER]

[Option 2: Verarbeitung außerhalb EU in einem Land mit Angemessenheitsbeschluss]

- (1) Die Parteien werden personenbezogene Daten im Rahmen der Durchführung des Projekts ausschließlich in den Mitgliedsstaaten der Europäischen Union oder in einem anderen Staat verarbeiten, der Partei des Vertrags über den Europäischen Wirtschaftsraum ist bzw. für das ein Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DS-GVO vorliegt.
- (2) Absatz 1 gilt für den Einsatz von Auftragsverarbeitern gemäß § 11 entsprechend.

[ODER]

[Option 3: Verarbeitung außerhalb EU/EWR in einem Land ohne Angemessenheitsbeschluss]

- (1) Eine Verarbeitung von personenbezogenen Daten außerhalb von EU/EWR bzw. einem Land ohne Angemessenheitsbeschluss gemäß Art. 45 DS-GVO ist nur dann zulässig, wenn die Voraussetzungen der Art. 44 ff. DS-GVO eingehalten werden.
- (2) Die Partei [XY] [jeweilige Partei im Drittland] verpflichtet sich zu keiner Zeit eine Re-Identifizierung der bei Ihm gespeicherten pseudonymisierten Daten durchzuführen. Zudem wird diese eine Kontaktaufnahme während und nach dem Abschluss der Studie zu den Studienteilnehmern ausdrücklich unterlassen, sofern in Anlage 1 nichts Anderes geregelt ist
- (3) Die Partei [XY] [jeweilige Partei im Drittland] ist verpflichtet, alle personenbezogenen Daten nach Ablauf der Verarbeitungstätigkeit – wie in dieser Vereinbarung beschrieben – an Partei 1 zurückzugeben oder zu löschen sofern keine gesetzlichen Aufbewahrungsfristen entgegenstehen.
- (4) Im Falle einer behördlichen Aufforderung zur Herausgabe von personenbezogenen Daten im Rahmen des Projektes, welche bei der Partei [XY] [jeweilige Partei im Drittland] gespeichert sind, verpflichtet sich Partei [XY] [jeweilige Partei im Drittland] eine offizielle Herausgabeanforderung bzw. einen offiziellen Beschluss zu verlangen. Weiterhin ist diese Partei verpflichtet alle zumutbaren und angemessenen Rechtsmittel gegen eine offizielle Herausgabeanforderung bzw. einen Beschluss einzulegen. Ferner verpflichtet sich die Partei [XY] [jeweilige Partei im Drittland] Partei 1 unverzüglich zu informieren. Dies gilt auch für den Fall, dass ein Zugriff auf personenbezogene Daten erst nachträglich bemerkt wird.
- (5) Aufgrund des Sitzes der Partei [XY] [jeweilige Partei im Drittland] in einem Land außerhalb der EU/EWR bzw. Land ohne Angemessenheitsbeschluss und der damit verbundenen Übermittlung von personenbezogenen Daten, verpflichten sich die Parteien zum Abschluss der von der EU-Kommission genehmigten Standardvertragsklauseln im Sinne des Art. 46 Abs. 2 c) DS-GVO, um ein angemessenes Datenschutzniveau beim Empfänger sicherzustellen.
- (6) Absatz 1 gilt für den Einsatz von Auftragsverarbeitern gemäß § 11 entsprechend.

§ 3 Verantwortlichkeit

- (1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Ziff. 7 DS-GVO).
- (2) Die Verarbeitungen von personenbezogenen Daten im Eigeninteresse des Auftragnehmers sind nur mit schriftlicher Zustimmung des Auftraggebers zulässig. Dabei stellt der Auftragnehmer sicher, dass für die jeweilige Verarbeitung eine Rechtsgrundlage – für welche der Auftragnehmer verantwortlich ist – gegeben ist. Der Auftragnehmer gewährleistet auch, dass für die ggf. erforderliche Offenlegung von personenbezogenen Daten vom Auftraggeber an den Auftragnehmer hinsichtlich einer im Eigeninteresse des Auftragnehmers vorzunehmenden Verarbeitung eine Rechtsgrundlage gegeben ist.
- (3) Der Auftragnehmer muss gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
- (4) Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

§ 4 Dauer des Auftrags

- (1) Die Dauer des Auftrags ist in § ... des Hauptvertrags zwischen Auftraggeber und Auftragnehmer geregelt, sofern sich aus den Bestimmungen dieses AV-Vertrages nicht etwas Anderes ergibt.

Die Vertragsparteien sind zu einer außerordentlichen Kündigung aus wichtigem Grund berechtigt. Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen AV-Vertrages z. B. bei Beendigung des vorliegenden Vertragsverhältnisses, keine (weitere) Auftragsverarbeitung durchgeführt werden darf.

§ 5 Weisungsbefugnis des Auftraggebers

- (1) Der Umgang mit den personenbezogenen Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). Der Auftragnehmer unterrichtet in derartigen Situationen den Auftraggeber unverzüglich vor Beginn der Verarbeitung über diese entsprechenden rechtlichen Anforderungen, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Auftraggeber behält sich im Rahmen der in diesem AV-Vertrag getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann.
- (2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
- (3) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format (bspw. E-Mail). Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
- (4) Ansprechpartner (weisungsberechtigte Personen) des Auftraggebers sind der folgenden Tabelle zu entnehmen:

Nr.	Name, Vorname	Funktion beim Auftraggeber	Kontakt (Telefon und E-Mail)
1			
2			

§ 6 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen des Auftrages und nach Weisungen des Auftraggebers.
- (2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht

wird. Er wird alle erforderlichen technischen und organisatorischen Maßnahmen zur angemessenen Sicherung der personenbezogenen Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Anforderungen der entsprechenden datenschutzrechtlichen Bestimmungen entsprechen; diese Maßnahmen muss der Auftragnehmer auf Anfrage dem Auftraggeber und ggfs. Aufsichtsbehörden gegenüber nachweisen. Dieser Nachweis beinhaltet insbesondere die Umsetzung der aus Art. 32 DS-GVO resultierenden Maßnahmen.

Die technischen und organisatorischen Maßnahmen unterliegen dem Stand der Technik. Insoweit ist es dem Auftragnehmer gestattet, alternative, nachweislich adäquate Maßnahmen umzusetzen. Dabei muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren. Eine Darstellung dieser technischen und organisatorischen Maßnahmen erfolgt in der beigefügten **Anlage 1** zu diesem Vertrag. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

- (3) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein aussagekräftiges und aktuelles Datenschutz- und Sicherheitskonzept, gemäß BSI-Grundschutz oder einem anderen anerkannten Standard für diese Auftragsverarbeitung zur Verfügung.
- (4) Der Auftragnehmer selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DS-GVO. Er stellt auf Anforderung dem Auftraggeber die für die Übersicht nach Art. 30 DS-GVO notwendigen Angaben zur Verfügung. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.
- (5) Der Auftragnehmer führt ergänzend zu Abs. (3) eine Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO, für die bei Ihm im Auftrag durchgeführte Verarbeitungstätigkeit, durch, sofern dies notwendig ist.
- (6) Der Auftragnehmer unterstützt den Auftraggeber bei einer von diesem durchzuführenden Datenschutzfolgenabschätzung mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde unterstützt der Auftragnehmer den Auftraggeber auch hierbei.
- (7) Die Verarbeitung von personenbezogenen Daten in Privatwohnungen (Telearbeit, Home-office etc.) durch den Auftragnehmer bedarf der vorherigen Zustimmung des Auftraggebers. Die zu treffenden technischen und organisatorischen Maßnahmen zur Wahrung des erforderlichen Sicherheitsniveaus und die sich daraus ergebenden besonderen Geheimhaltungspflichten werden mit dem Auftragnehmer abgestimmt.
- (8) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln.
- (9) Als Datenschutzbeauftragter ist beim Auftragnehmer derzeit
[Name, Kontaktdaten] benannt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen. Der Auftragnehmer gewährleistet, dass die

Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 37 ff. DS-GVO erfüllt werden. Sofern kein Datenschutzbeauftragter beim Auftragnehmer benannt ist, nennt der Auftragnehmer dem Auftraggeber einen Ansprechpartner.

- (10) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich - spätestens innerhalb von 24 Stunden - bei der Kenntnis oder einem begründeten Verdacht von erheblichen Unregelmäßigkeiten im Rahmen der Datenverarbeitung bei ihm oder beauftragten Dritten oder bei Verstößen des Auftragnehmers - oder der bei ihm im Rahmen des Auftrags beschäftigten Personen - gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen. Den Auftragnehmer trifft insoweit eine Nachforschungspflicht, wenn ihm Anhaltspunkte hierfür bekannt werden. Er trifft nachweislich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen, spricht sich hierzu unverzüglich mit dem Auftraggeber ab und macht Vorschläge für weitere zu treffende notwendige Maßnahmen. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten gegenüber der jeweiligen Aufsichtsbehörde bzw. gegenüber den Betroffenen nach Art. 33, 34 DS-GVO. Eine Prüfung des Auftragnehmers, ob eine eigene Verpflichtung zur Meldung an eine Aufsichtsbehörde vorliegt, bleibt hiervon unberührt.
- (11) Soweit ein Betroffener einen Antrag auf Wahrnehmung der ihm zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend machen sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
- (12) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Die gesetzlichen Aufbewahrungs- bzw. Nachweispflichten des Auftragnehmers bleiben unberührt.
- (13) Der Auftragnehmer unterstützt den Auftraggeber bei der fristgemäßen Erfüllung der Ansprüche betroffener Personen wie etwa bei Auskunftsansprüchen, Berichtigungs- und Löschbegehren sowie der Geltendmachung eines Widerrufs einer Einwilligung. Sofern dem Auftragnehmer die Daten nur pseudonym vorliegen, erfolgt die entsprechende Kommunikation ausschließlich pseudonym.
- (14) Der Auftragnehmer informiert den Auftraggeber unverzüglich über die Ankündigung oder Durchführung von Kontrollen und Ermittlungsmaßnahmen durch die Aufsichtsbehörden.
- (15) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.
- (16) Sollten die personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten ausschließlich beim Auftraggeber als Verantwortlichem und „Herr der Daten“ im Sinne der DS-GVO liegt. Der Auftragnehmer legt in diesen Fällen unverzüglich verhältnismäßige Rechtsmittel – ggfs. mit aufschiebender Wirkung - ein, wenn auf personenbezogene Daten zugegriffen werden soll bzw. eine Herausgabe verlangt wird.

- (17) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten, außer in den Fällen des § 3 Abs. 2 dieses AV-Vertrages, für keine anderen, - insbesondere nicht für eigene Zwecke - als die der Vertragserfüllung und setzt auch keine Mittel zur Verarbeitung ein, die nicht vom Auftraggeber zuvor genehmigt wurden. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Der Auftragnehmer sichert zu, dass die für den Auftraggeber verarbeiteten personenbezogenen Daten von sonstigen Datenbeständen strikt getrennt werden.
- (18) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren, zu dokumentieren und in geeigneter Weise gegenüber dem Auftraggeber auf Anforderung nachzuweisen.

§ 7 Pflichten des Auftraggebers

- (1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z. B. durch Einholung von Einwilligungserklärungen für die Verarbeitung der personenbezogenen Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen zulässig erbringen kann.
- (2) Der Auftraggeber hat den Auftragnehmer zu informieren, wenn er bei der Prüfung der Vertragsverpflichtungen des Auftragnehmers Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt und fordert zu einer unverzüglichen Klärung der Fehler bzw. Unregelmäßigkeiten auf.
- (3) Der Auftraggeber ist hinsichtlich der vom Auftragnehmer eingesetzten und vom Auftraggeber genehmigten Verfahren zur automatisierten Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich und hat – neben der eigenen Verpflichtung des Auftragnehmers – ebenfalls die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.
- (4) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

§ 8 Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber hat das Recht, in Absprache mit dem Auftragnehmer Überprüfungen durchzuführen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb ohne Störung des Betriebsablaufs persönlich oder durch einen sachkundigen Dritten, der nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen darf, von der Einhaltung der vereinbarten Regelungen zu überzeugen.
- (2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

Der Nachweis solcher Maßnahmen erfolgt nach den Vorgaben von Art. 40 DS-GVO ff.

- (3) Werden dem Auftraggeber Tatsachen hinsichtlich einer Gefährdung der datenschutzrechtlichen Gewährleistungsziele bekannt oder liegt ein hinreichender Verdacht eines Verstoßes des Auftragnehmers - oder der bei ihm im Rahmen des Auftrags beschäftigten Personen - gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Prüfung auch mit kurzfristiger Ankündigung vorgenommen werden, sofern dies dem Auftraggeber möglich ist. Eine Störung des Betriebsablaufs beim Auftragnehmer sollte hierbei, wenn möglich, vermieden werden.
- (4) Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftraggeber im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags wird vom Auftragnehmer unterstützt. Insbesondere verpflichtet sich der Auftragnehmer, dem Auftraggeber auf schriftliche Anforderung - wobei dieses Erfordernis durch eine einfache Textform (z.B. per E-Mail) gewahrt wird - innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.
- (5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn bei der Prüfung Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen festgestellt werden.

§ 9 Berichtigung, Einschränkung der Verarbeitung, Löschung und Rückgabe von Datenträgern

- (1) Während der laufenden Beauftragung berichtigt, schränkt ein oder löscht bzw. vernichtet der Auftragnehmer die vertragsgegenständlichen Daten nur auf Anweisung des Auftraggebers, es sei denn, es liegt eine gesetzliche Verpflichtung des Auftragnehmers vor. In diesen Fällen hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig zu informieren.
- (2) Sofern eine Vernichtung oder Löschung während der laufenden Beauftragung vorzunehmen ist, übernimmt der Auftragnehmer die nachgewiesene datenschutzkonforme Vernichtung von Datenträgern und sonstiger Materialien, auf denen personenbezogene Daten verarbeitet sind, nur aufgrund entsprechender Einzelbeauftragung durch den Auftraggeber. Dies gilt nicht, sofern im Hauptvertrag bereits eine entsprechende Regelung getroffen worden ist.
- (3) In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung durch den Auftragnehmer bzw. Übergabe an den Auftraggeber.
- (4) Nach Abschluss der Erbringung der Verarbeitungsleistungen muss der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder löschen, vernichten und/ oder diesem zurückgeben oder -übersenden bzw. dem Auftraggeber die Möglichkeit zum Zugriff und zur Sicherung sämtlicher in seinen Besitz gelangter Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände einräumen, sofern nicht nach dem Unionsrecht oder dem für den Auftragnehmer geltendem nationalen Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Im Falle einer Löschpflicht ist das Protokoll der Löschung auf Anforderung vorzulegen. Vom Auftraggeber an den Auftragnehmer überlassene Datenträger und deren Kopien sind nach Vertragsende in jedem Fall an den Auftraggeber herauszugeben.
- (5) Soweit ein Transport eines Speichermediums - auf den personenbezogenen Daten des Auftraggebers gespeichert sind - unverzichtbar ist, wird der Auftragnehmer angemessene

Maßnahmen zu dessen Schutz, insbesondere gegen Entwendung, unbefugtem Zugriff, Kopieren oder Verändern, treffen.

- (6) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.
- (7) Der Auftraggeber kann jederzeit, d. h. sowohl während der Laufzeit als auch nach Beendigung des Vertrages, die Berichtigung, Löschung, Verarbeitungseinschränkung und Herausgabe von personenbezogenen Daten durch den Auftragnehmer im Rahmen des rechtlich Zulässigen verlangen und informiert den Auftragnehmer, wenn vertragsgegenständliche personenbezogene Daten berichtigt, gelöscht wurden oder deren Verarbeitung beim Auftraggeber eingeschränkt wurde, sofern diese Änderungen auch den Auftragnehmer im Rahmen seiner Vertragserfüllung betreffen.

§ 10 Unterauftragnehmer

- (1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der personenbezogenen Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
- (2) Der Auftragnehmer darf grundsätzlich schriftlich Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Folgende Konstellationen sind möglich:
 - a) ☐ Eine Unterbeauftragung ist unzulässig.
 - b) ☐ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu:

Firma Unterauftragnehmer	Anschrift/Land	Datenschutzniveau (EU ¹ / Angemessenheitsbeschluss ² / Drittland ³)	Leistung bzw. Angabe der Verarbeitung von Datenkategorien

- c) ☐ Die Auslagerung auf Unterauftragnehmer oder ☐ der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:

¹ Vgl. Liste der EU-Länder der Europäischen Union unter: https://europa.eu/european-union/about-eu/countries_de.

² Vgl. Auflistung der EU-Kommission unter: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

³ Die DS-GVO sieht für die Übermittlungen personenbezogener Daten in ein Land außerhalb der EU/des EWR besondere Regelungen vor, vgl. https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_4.pdf.

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
 - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
 - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.
- (3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- (4) Will der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR erbringen, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen (§ 2 Abs. 2) sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
- (5) Eine weitere Auslagerung durch Unterauftragnehmer
- ☐ ist nicht gestattet;
 - ☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
 - ☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

- (6) Der Auftragnehmer muss Unterauftragnehmer gewissenhaft und unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen auswählen.
- (7) Ist der Auftragnehmer im Sinne dieser Vereinbarung befugt, die Dienste eines Unterauftragnehmers in Anspruch zu nehmen, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem Unterauftragnehmer dieselben Pflichten auferlegt, die in dieser Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern. Hierbei müssen ferner hinreichend Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt. Dem Auftraggeber sind im Unterauftragsverarbeitungsvertrag gegenüber dem Unterauftragnehmer unmittelbar sämtliche Kontrollrechte gemäß diesem AV-Vertrag einzuräumen.
- (8) Durch schriftliche Aufforderung - wobei dieses Erfordernis durch eine einfache Textform (z.B. per Email) gewahrt wird - ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.
- (9) Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers.

- (10) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (§ 8 dieser Vereinbarung) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

§ 11 Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts -gleich aus welchem Rechtsgrund- an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.

§ 12 Haftung

- (1) Für alle datenschutzrechtlichen Haftungsfragen der Vertragsparteien gelten die gesetzlichen Bestimmungen, insbesondere die DS-GVO. Soweit Dritte Ansprüche gegen den Auftraggeber geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftragnehmers gegen eine ihn unmittelbar treffende gesetzliche Datenschutzverpflichtung haben, stellt der Auftragnehmer den Auftraggeber von diesen Ansprüchen auf erstes Anfordern frei.
- (2) Der Auftragnehmer trägt die Beweislast dafür, dass etwaige Schäden nicht auf einem von ihm zu vertretenden Umstand beruhen, soweit die jeweilige Ursache in der Verarbeitung von Daten, für deren Verarbeitung der Auftraggeber der Verantwortliche ist, in der Zuständigkeitssphäre des Auftragnehmers liegen.
- (3) Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.
- (4) Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er
- a. seinen ihm speziell durch die DS-GVO auferlegten Pflichten nicht nachgekommen ist oder
 - b. unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.
- (5) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

§ 13 Schriftformklausel

Änderungen und Ergänzungen dieses AV-Vertrages und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Regelungen handelt. Das Schriftformerfordernis gilt auch für den Verzicht auf dieses Formerfordernis.

§ 14 Salvatorische Klausel

- (1) Sollten sich einzelne Bestimmungen dieses AV-Vertrages ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.
- (2) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.
- (3) Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedacht Werdens vereinbart worden wären.
- (4) Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, die den Schutz der personenbezogenen Daten im Sinne dieses Vertrages am besten gewährleistet.

§ 15 Rechtswahl, Gerichtsstand

- (1) Es gilt deutsches Recht.
- (2) Gerichtsstand ist der Sitz des Auftraggebers.

Für das NUM:

Für den Auftragnehmer:

Ort, Datum, Unterschrift

Ort, Datum, Unterschrift

Anlagen:

Anlage 1 Nachweis der technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs.3 S.2 lit. c i.V.m. Art. 32, Art. 30 Abs.2 lit. d und g DS-GVO

Anlage 1 zum AV-Vertrag: Nachweis der technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S.2 lit. c i.V.m. Art. 32, Art. 30 Abs. 2 lit. d und g DS-GVO

HINWEIS: Bitte beschreiben Sie die Maßnahmen, sofern zutreffend. Bitte löschen Sie NICHT die Vorgaben zu nicht zutreffenden Maßnahmen.

1. Sicherstellung der Rechtmäßigkeit der Datenverarbeitung

Die Maßnahmen sollen primär die Einhaltung der Gewährleistungsziele Vertraulichkeit, Transparenz, Zweckbindung, Datenminimierung, Nichtverkettabarkeit und Authentizität sicherstellen. Dabei sind auch die Rechte der betroffenen Personen auf Information und nach Art. 7 Abs. 3, 15 ff. DS-GVO sicherzustellen, einschließlich der Schadensminimierungsmaßnahmen und Informationsverpflichtungen gegenüber der Verantwortlichen

☐ Alle Mitarbeitenden sind datenschutzrechtlich geschult und gemäß der in dem u. g. Datenschutzmanagement geltenden Richtlinien mit der Wahrung und Umsetzung der Rechte der Betroffenen einschließlich des Umgangs mit Verletzungen von Datenschutzrechts bekannt.	☐ Verkehrsdaten werden dem Stand der Technik entsprechend verschlüsselt und so vor unautorisierter Kenntnisnahme und / oder Veränderung geschützt, z. B. gemäß den technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI, z. B. BSI TR-02102).
☐ Eine über den Auftragsverarbeitungsvertrag hinausgehende Verarbeitung im eigenen Interesse des Auftragnehmers ist den betroffenen Personen transparent bekannt gemacht worden.	☐ Bei auftragsgemäßer Erhebung von Daten: explizite Sensibilisierung, dass nur die erforderlichen Daten erhoben und eingesehen werden.
☐ Datenschutzfreundliche Voreinstellungen der eingesetzten Systeme zur Datenverarbeitung.	☐ Eine Übertragung von personenbezogenen Daten auf private Endgeräte oder Systeme ist technisch und / oder organisatorisch unterbunden.
☐ Es liegt ein fortlaufend aktualisiertes Berechtigungskonzept vor, das sicherstellt, dass nur die Mitarbeitenden und auch nur im jeweils erforderlichen Umfang auf die für ihre Aufgabenerfüllung erforderlichen Daten Zugriff erlangen.	☐ Ein Löscho- / Sperrkonzept liegt vor: Nicht mehr erforderliche Daten werden gelöscht oder gesperrt.
☐ Bei Audiodateien, die transkribiert werden: Die Audiodateien werden datenschutzgerecht gelöscht, unverzüglich dem eine Transkription erfolgt ist und die Daten validiert worden sind.	☐ Videodateien (z. B. Überwachung) werden nach Ablauf von (bitte geben Sie eine Zahl ein) Tagen datenschutzgerecht gelöscht.

Weitere Maßnahmen:

☐

☐

2. Zutrittskontrolle

Diese Maßnahmen sollen die Einhaltung der Gewährleistungsziele der Vertraulichkeit, Rechtmäßigkeit, Transparenz, Integrität, Intervenierbarkeit sowie der Nichtverkettabarkeit sicherstellen. Sie betreffen vorrangig Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Gebäuden und Räumen, in denen Daten / Datenträger aufbewahrt werden, oder Datenverarbeitungsanlagen, mit denen schützenswerte Daten verarbeitet oder genutzt werden, enthalten sind, zu verwehren bzw. zu detektieren. Als Maßnahmen zur Zutrittskontrolle können unter anderem automatische Zutrittskontrollsysteme wie Schließsysteme mittels Chipkarten und Transpondern, Kontrolle des Zutritts durch Pförtnerdienste und, ergänzend dazu, Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschlossenen Schränken (Racks) zu schützen. Darüber hinaus ist es sinn-

voll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z. B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit oder auch das Schließen von Fenstern vorsieht) zu unterstützen.

☐ Sicherheitsschlösser	☐ Geordneter Prozess zur Vergabe und zum Entzug von Zutrittsrechten
☐ Regelmäßige Prüfung von Zutrittsrechten	☐ Alarmanlage(n) in für die vertragliche Leistung relevanten Bereichen
☐ Pförtnerdienst in für die vertragliche Leistung relevanten Bereichen	☐ Videoüberwachung in für die vertragliche Leistung relevanten Bereichen
☐ Dienstanweisung zum Verschließen von Räumen bei Abwesenheit	

Weitere Maßnahmen

- ☐
- ☐

3. Zugangskontrolle

Diese Maßnahmen sollen die Einhaltung der Gewährleistungsziele der Vertraulichkeit, Verfügbarkeit, Authentizität, Rechtmäßigkeit, Transparenz, Integrität, Intervenierbarkeit sowie der Nichtverkettbarkeit sicherstellen. Sie betreffen in Abgrenzung zur Zutrittskontrolle den Zugang zu Daten und Datenträgern direkt. Um Unbefugten den Zugang zu Daten oder Datenträgern zu verwehren ist mindestens eine Authentifizierung am System vorzusehen.

Möglichkeiten der Zugangskontrolle sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, automatische Sperre des Bildschirms nach einer angemessenen Spanne von Inaktivität, Verpflichtung der Nutzenden, dessen ungeachtet auch manuell den Bildschirm zu sperren, wenn der Arbeitsplatz verlassen wird oder der Einsatz von Chipkarten zur Anmeldung. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern z. B. Dienstanweisungen zur sichtgeschützten Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl von Passwörtern oder dergleichen.

☐ Lagerung von Datenträgern mit personenbezogenen Daten erfolgt in abschließbaren, zerstörungssicheren Schränken / Anlagen mit dokumentierter Schlüsselvergabe.	☐ Dienstanweisung zum sicherem Umgang mit mobilen Datenträgern und Geräten.
☐ Bedarfsgemäße Zugangssteuerung.	☐ Soweit ausreichend für den jeweiligen Zweck: Zugang zu schützenswerten Daten pseudonymisiert / geschwärzt.
☐ Zugang zu IT-Systemen erfolgt mit angemessenem Passwortschutz, der der Sensitivität der verarbeiteten Daten entspricht.	☐ Alarmsystem bei (versuchtem) unbefugten Zugang zu elektronischen Daten.
☐ Zwei Faktor-Authentifizierung bei Zugang zu elektronisch gespeicherten sensiblen personenbezogenen Daten auf mobilen Datenträgern, oder zu personenbezogenen Daten, die vom Auftraggeber als besonders schützenswert gekennzeichnet werden.	☐ Schutzsoftware (z. B. Anti-Schadsoftware-Lösungen, Firewalls etc.) wird dem Stand der Technik entsprechend eingesetzt. Es wird auf die entsprechenden Bausteine des BSI-Grundschutz-Kompendiums verwiesen.
☐ Die Verschlüsselung erfolgt nach dem Stand der Technik (bspw. BSI-TR-02102).	

Weitere Maßnahmen

- ☐
- ☐

4. Zugriffskontrolle

Die Maßnahmen sollen die Einhaltung der Gewährleistungsziele: Vertraulichkeit, Transparenz, Rechtmäßigkeit, Integrität, Authentizität und, Intervenierbarkeit gewährleisten.

Sie sollen gewährleisten, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Weiterhin sind geeignete Prozesse, Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf dem aktuellen Stand zu halten (z. B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Benutzerkonten mit erhöhten Berechtigungen (Administratorinnen und Administratoren) zu richten.

☐ Angemessener Sichtschutz für Akten und Dokumente sowie leicht einsehbare Monitore.	☐ Dienstanweisung, die vorsieht, dass Datenanzeigen vor Sichtung durch Unbefugte zu schützen sind und der Arbeitsplatz durch eine passwortgeschützte Bildschirmsperre für Unbefugte zu sperren ist.
☐ Reduzierung der Verwendung mobiler Datenträger mit sensiblen Daten auf das im Einzelfall zu begründende erforderliche Maß (bspw. Dienstanweisung, kontrollierte Bereitstellung von mobilen Endgeräten).	☐ Administrations- und Wartungstätigkeiten der zur Datenverarbeitung genutzten mobilen Endgeräte erfolgen zentral durch eigene Mitarbeitende – Bitte Begründung Sie, wenn dies nicht vorliegt:
☐ Bei Nutzung mobiler Datenträger: erfolgt verschlüsselt nach dem Stand der Technik (bspw. CD-ROM, externe Massenspeicher wie USB-Sticks oder externe Festplatten).	☐ Dienstanweisung zur sicheren Aufbewahrung der vertragsgegenständlichen Datenträger.
☐ Es liegt ein vollständiges Kryptografie-Konzept vor, welches sicherstellt, dass alle schützenswerten Daten auf mobilen Datenträgern ausschließlich verschlüsselt gespeichert und übertragen werden.	

Weitere Maßnahmen

- ☐
- ☐

5. Trennungskontrolle

Die Maßnahmen sollen primär sicherstellen, dass die Gewährleistungsziele der Transparenz, der Rechtmäßigkeit / Erforderlichkeit sowie der Nichtverkettbarkeit von personenbezogenen Daten eingehalten werden.

Schützenswerte Daten anderer Auftraggeber oder die zu eigenen Zwecken verarbeiteten Daten sind von denen, die im Rahmen dieses Auftragsvertragsvertrages verarbeitet werden, zu trennen.

Zu unterschiedlichen Zwecken erhobene Daten sollen getrennt verarbeitet werden. Insbesondere sollen schützenswerte Daten des Auftraggebers nicht nachteilig von Datenschutz- oder Sicherheitsvorfällen betreffend die Daten des Auftragnehmers oder anderer Kunden in Mitleidenschaft gezogen werden. Dieses kann beispielsweise durch logische oder physikalische Trennung der Daten gewährleistet werden. Jeder Versuch einer nicht gerechtfertigten Re-Identifizierung von pseudonymen Daten ist technisch und / oder organisatorisch zu unterbinden. So sollte weder ein Kontakt betroffenen Personen hergestellt werden.

☐ Mandantentrennung	☐ Der De-Pseudonymisierungsschlüssel liegt nur bei der Auftraggeberin.
☐ Eine Re-Identifizierung ist nur dem Auftraggeber möglich.	☐ Sofern zutreffend: Anonymisierung erfolgt nach anerkannten Regeln.

☐ Durch ein Berechtigungskonzept ist organisatorisch und technisch sichergestellt, dass Zugriffe auf Dateien nur durch dazu befugte Personen und nur im jeweils erforderlichen Umfang erfolgt.	☐ Angemessene Protokollierung auf IT-Systemen und angemessene Aufbewahrungsdauer der Zugriffe auf schützenswerte Daten. Mit Hilfe der Protokolle muss es möglich sein Datenschutz- und Informationssicherheitsvorfälle entdecken und nachvollziehen zu können.
☐ Datenschutzfreundliche Voreinstellungen der Systeme.	☐ Dienstanweisung zum Verbot der Datenübertragung auf private Endgeräte oder Datenträger.

Weitere Maßnahmen

- ☐
- ☐

6. Weitergabekontrolle

Die Maßnahmen sollen primär die Einhaltung der Gewährleistungsziele der Verfügbarkeit, der Vertraulichkeit, der Rechtmäßigkeit / Erforderlichkeit, Transparenz, Verfügbarkeit, Intervenierbarkeit sowie der Nichtverkettbarkeit gewährleisten. Personenbezogene Daten dürfen nicht an unbefugte Personen weitergegeben werden. Bei der Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern dürfen diese nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es muss überprüft und festgestellt werden können, an welchen Stellen eine Übermittlung personenbezogener Daten erfolgt. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z. B. Verschlüsselungstechniken (z. B. Virtual Private Network, VPN) eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

☐ Standardmäßige Protokollierung der Weitergabe (Ort, Datum, Geber und Empfänger sowie Zweck) von Daten(-trägern) (bspw. Papierdokumente, Sticks, CD, Festplatten u. a.).	☐ Ausreichende physische Sicherung von analogen Datenträger vor unbefugter Kenntnisnahme (bspw. verschlossene Vorrichtungen).
☐ Versendung von Datenträgern per Einschreiben oder in beleghafter Form.	☐ Herausgabe von Datenträgern und Biomaterialproben erfolgt nur bei beleghaftem Nachweis der Berechtigung des Empfängers (bspw. Antragsverfahren, Antragsformulare bei Zugriffswunsch).
☐ Datenschutzfreundliche Voreinstellungen der Systeme wie z.B. individuelles Aktivieren von Aufnahme-funktionen Audio und Bild erforderlich, bei einer Datenübertragung ist die Übertragung von Identifikatoren gesondert zu aktivieren.	☐ Datenherausgabe in ein Drittland erfolgt nur nach gesonderter Prüfung der Rechtmäßigkeitsvoraussetzungen und Freigabe durch den Auftraggeber.
☐ Dienstanweisungen und ausreichende Belehrungen / Sensibilisierungen für den datenschutzkonformen und sicheren Umgang mit Datenträgern, die Mitarbeitende mit sich führen (bspw. Arbeitslisten mit schützenswerten Daten, Papierakten, mobile Endgeräte).	☐ Standardmäßige Protokollierung der Weitergabe/Übertragung elektronischer Daten.
☐ Angemessen verschlüsselte Übertragung elektronischer Daten nach dem Stand der Technik (z. B. gemäß BSI-TR-02102).	☐ Dienstanweisung zum Verbot der Datenübertragung auf private Endgeräte oder Datenträger.

Weitere Maßnahmen

- ☐
- ☐

7. Eingabekontrolle

Die Maßnahmen sollen primär die Einhaltung der Gewährleistungsziele der, Integrität, Richtigkeit, Rechtmäßigkeit / Transparenz, Authentizität, Verfügbarkeit gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Die Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z. B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Ereignisse protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass / Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfinden muss.

☐ Berechtigungskonzept unterscheidet mindestens in Lese – und Schreibrechte.	☐ Eine Eingabe von nicht berechtigten Personen ist ausgeschlossen: ☐ technisch ☐ organisatorisch
☐ Änderungen und Löschungen von Dateien in elektronischen Datenverarbeitungssystemen werden protokolliert – bitte geben Sie an, wie lange die Protokolle aufbewahrt werden:	☐ Dienstanweisung zur Protokollierung von Änderungen in nicht elektronischen Datenverarbeitungssystemen.

Weitere Maßnahmen

- ☐
- ☐

8. Verfügbarkeitskontrolle

Die Maßnahmen sollen primär die Einhaltung der Gewährleistungsziele der Verfügbarkeit, Transparenz und Intervenierbarkeit gewährleisten. Personenbezogene Daten müssen gegen zufällige Zerstörung oder Verlust geschützt sein. Dazu gehören Maßnahmen zum Diebstahlschutz, unterbrechungsfreie Stromversorgungsanlagen, Klimaanlage, Brandschutzmaßnahmen, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

☐ Die Vernichtung von Datenträgern wird protokolliert.	☐ Backup- und Wiederherstellungskonzept nach dem Stand der Technik, das auch nachvollziehbare Wiederherstellungsübungen beinhaltet.
☐ Ein Notfallkonzept liegt vor. ☐ Für besonders hohe Anforderungen an die Verfügbarkeit gibt es ein Notfallmanagementsystem nach anerkannten Standards wie z. B. BSI 100-4, 200-4, ISO 22301 o. ä.	☐ Regelmäßige stichprobenartige Verfügbarkeitskontrollen für Datenträger.

Weitere Maßnahmen

- ☐
- ☐

9. Datenschutz-Management

Die Maßnahmen sollen die angemessene Umsetzung **aller** datenschutzrechtlichen Gewährleistungsziele bei dem Auftragnehmer sicherstellen. Auf Anfrage ist der Auftraggeber berechtigt, beleghafte Informationen zu den konkreten Maßnahmen zu erhalten, vgl. Haupt- AV-Vertrag

☐ Vorliegen eines datenschutzkonformen Lös- / Sperrkonzeptes.	☐ Passwortrichtlinie und deren technische Umsetzung / Durchsetzung.
☐ Regelmäßige, anlassunabhängige Durchführung von Audits (insb. Protokollauswertungen).	☐ Richtlinien zum Umgang mit der Wahrung der Rechte und Freiheiten betroffener Personen welche berücksichtigen

	☐ Eine rechtzeitige Information des Auftraggebers über Datenschutz- oder Informationssicherheitsvorfälle ist sichergestellt. Auch Verdachtsfälle sind unverzüglich zu melden. ☐ Richtlinien / Arbeitsanweisungen zum Umgang mit meldepflichtigen Datenpannen. ☐ Incident-Response-Management umfasst Alarm- und Warnfunktionen sowie Festlegung von Schadensminimierungsmaßnahmen, Zuständigkeiten und Abläufen sowie die Meldepflichten gegenüber der Aufsichtsbehörde sowie den Betroffenen.
☐ Führen eines Verzeichnisses von Verarbeitungstätigkeiten.	☐ Administratives Personal für Passwortverwaltung ist benannt und auf das notwendige Maß reduziert.
☐ Regelmäßige Schulungen der Mitarbeitenden zum Datenschutz und zur Informationssicherheit finden statt.	☐ Datenschutzbeauftragte/r benannt und erreichbar.
☐ für die Verarbeitungstätigkeit liegen Datenschutzkonzepte im Sinne der jeweils einschlägigen Rechtsvorschriften vor (z. B. Art. 32 DS-GVO, BDSG).	☐ Testverfahren für neue Verarbeitungstätigkeiten sind implementiert und finden nachvollziehbar statt.
☐ Für die Verarbeitungstätigkeit erfolgte eine Datenschutzfolgenabschätzung im Sinne von Art. 35 DS-GVO.	

Weitere Maßnahmen

☐

☐

10. Auftragskontrolle (Outsourcing an Dritte)

Es muss dafür gesorgt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Daher erfolgt keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers durch folgende **Mindestanforderungen**:

☐ Eindeutige Vertragsgestaltung	☐ Formalisiertes Auftragsmanagement
☐ Strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS)	☐ Vorabüberzeugungspflicht
☐ Nachkontrollen	

Sofern die Einhaltung nicht möglich sein sollte, begründen Sie bitte nachfolgend:

.....

Weitere Maßnahmen

☐

☐